Quantitative Risk Analysis: Challenges and Opportunities at NASA

Bill Vesely
Manager, Risk Assessment
Office of Safety and Mission Assurance
NASA Headquarters

Examples of Quantitative Risk Analyses

- NASA carries out a spectrum of QRAs
- Examples presented:
  - Space Shuttle PRA
  - DC-8 Project Risk Assessment
  - Software Development Risk Assessment
- These examples illustrate the challenges and opportunities for QRA

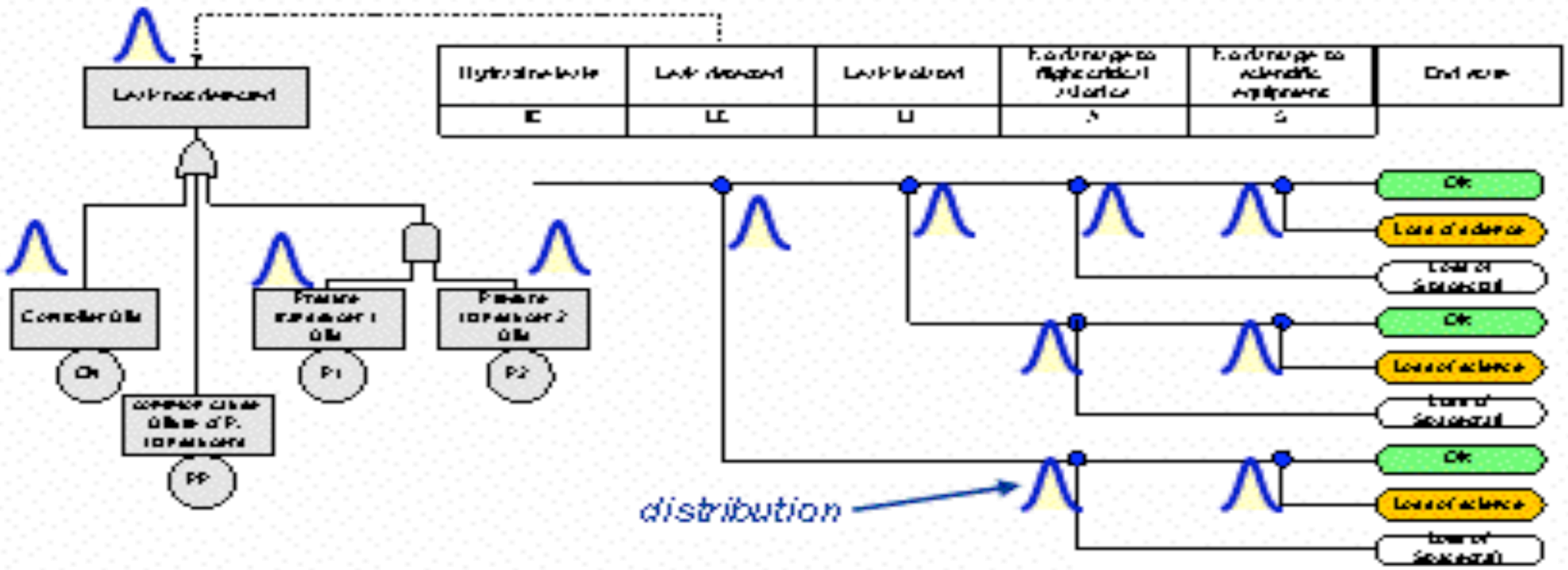
NASA Criteria for Selecting the Scope of a PRA (1)

CONSEQUENCE CATEGORY	**CRITERIA / SPECIFICS**		**NASA PROGRAM/PROJECT (Classes and/or Examples)**	**PRA SCOPE**
Human Safety and Health	Public Safety	Planetary Protection Program Requirement	Mars Sample Return Missions	**F**
		White House Approval (PD/NSC-25)	Nuclear Payloads (e.g., Cassini, Ulysses, Mars 2003)	**F**
		Space Missions with Flight Termination Systems	Launch Vehicles	**F**
	Human Space Flight		International Space Station	**F**
			Space Shuttle	**F**
			Orbital Space Plane/Space Launch Initiative	**F**
Mission Success (for non-human rated missions)	High Strategic Importance		Mars Program	**F**
	High Schedule Criticality		Launch Window (e.g., planetary missions)	**F**
	All Other Missions		Earth Science Missions (e.g., EOS, QUICKSCAT)	**L/S**
			Space Science Missions (e.g., SIM, HESSI)	**L/S**
			Technology Demonstration/Validation (e.g., EO-1, Deep Space 1)	**L/S**

1. NASA. July 12, 2004. *NASA Procedural Requirements*, *Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects.* NPR 8705.5

Mission Success Starts With Safety

Event- and Fault-Tree Scenario Modeling



Fault tree

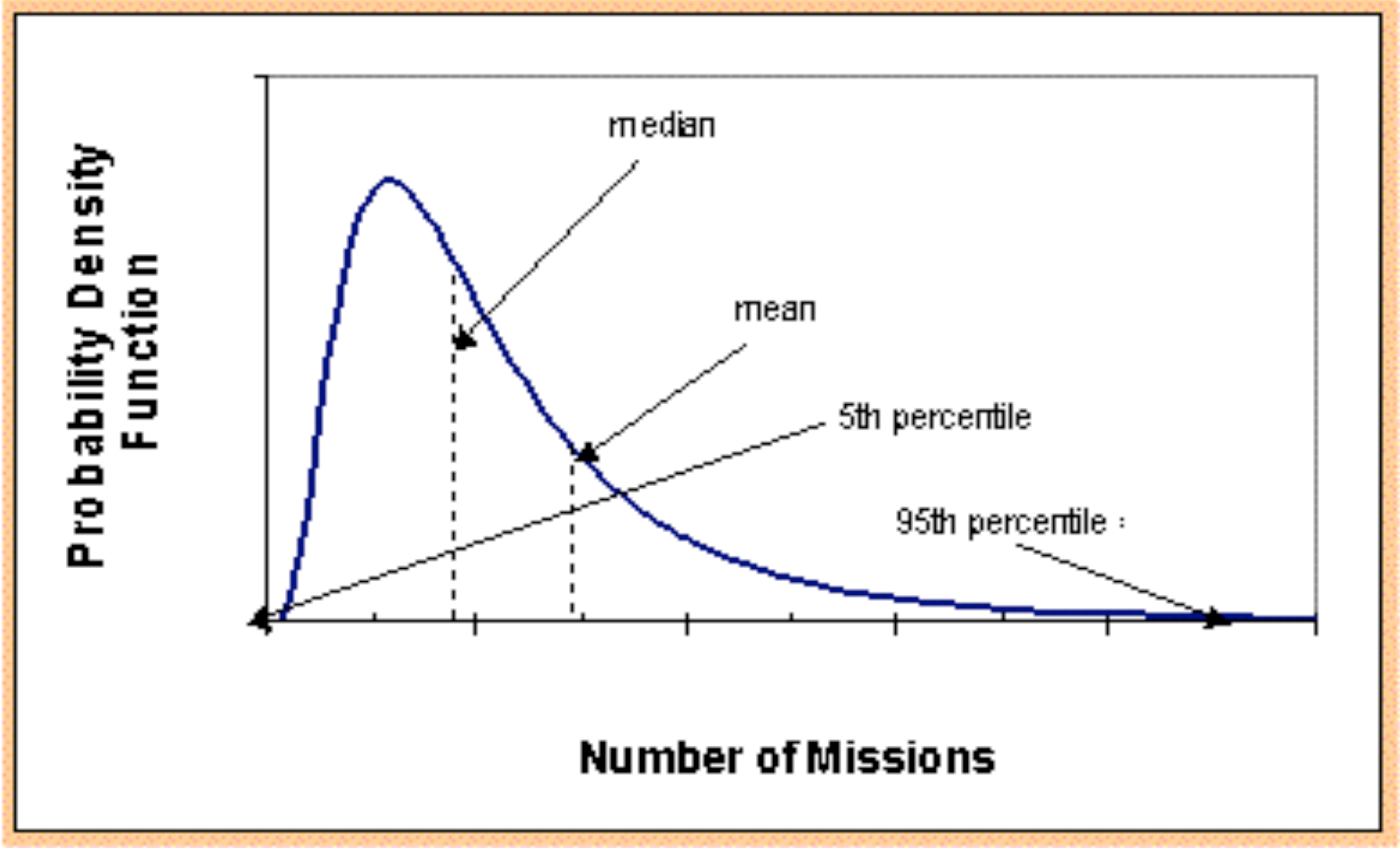
Event tree

General Features of the NASA Space Shuttle PRA

- ~ 5000 Event Trees
- ~ 100 Fault Trees
- ~ 6000 Basic Events
- ~ 2 Million Minimal Cutsets
- ~ 100 Off-line Supporting Models
- ~ Several Thousand Pages of Paper

Mission Success Starts With Safety

Probability Distribution for Number of Missions to Failure



Example Listing of Detailed Contributors to LOCV

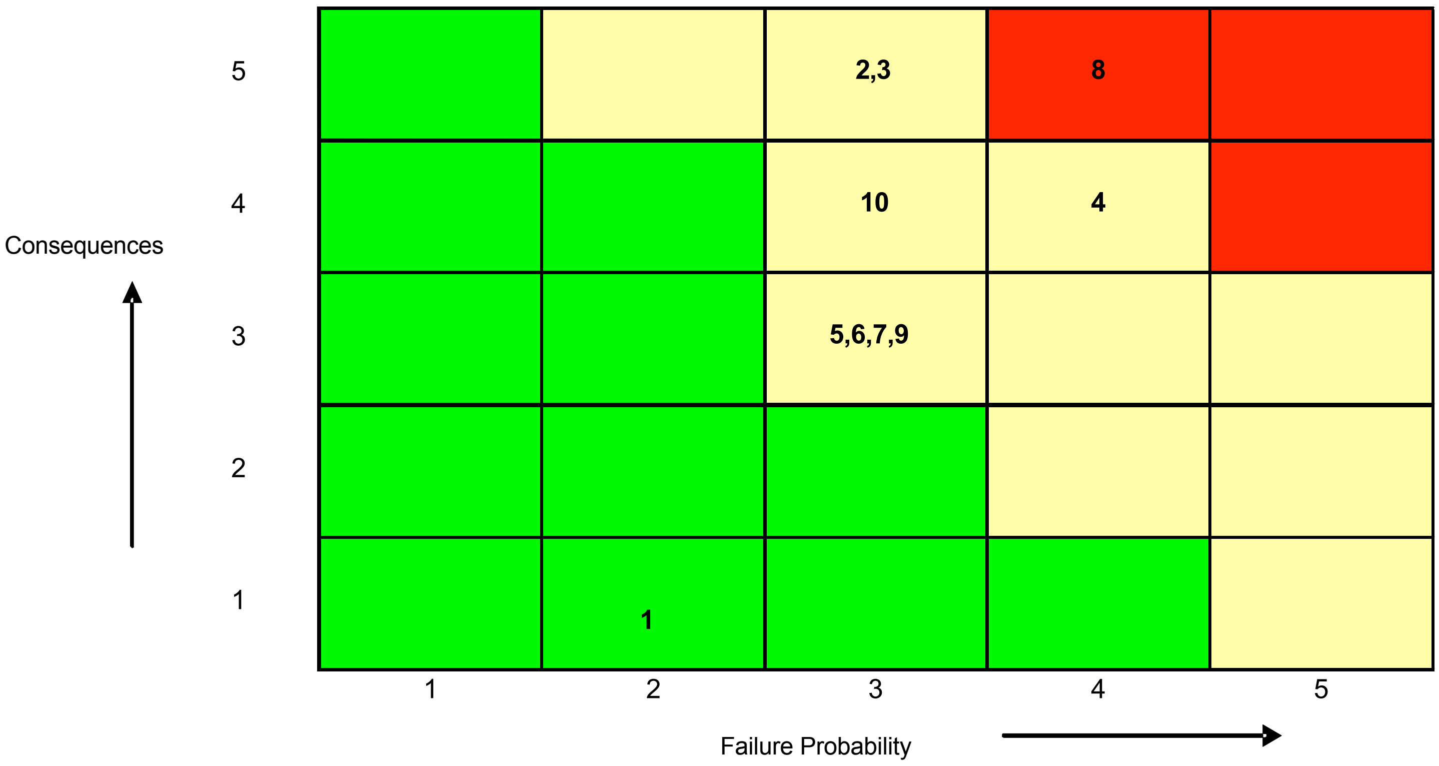
Cut No.	Description
1	LOCV Given Two Main Landing Gear Tires Fail
2	LOCV Due To Crew Failing To Deploy Landing Gear At Correct Time
3	LOCV Due To Failure Of Right Side Forward Mid Edge TPS Consists Of 624 Tiles
4	MPS Gaseous He Tanks Depressurize On Orbit Causing LOCV
5	MPS Liquid H2 Leak Causes LOCV
6	MPS Liquid O2 Leak Causes LOCV
7	LOCV Due To Failure Of Right Side TPS Under Crew Cabin, Consists Of 156 Tiles
8	LOCV Due To Failure Of Right Side Near Main Landing Gear (Aft) TPS, Consists Of 156
9	LOCV Due to Structural Failure of the Forward Booster Separation Motor Throat
10	LOCV Due to ET Separation and SSME Shutdown Sequence (Several sequences combined)
11	LOCV Due to Catastrophic Failure of the RSRM Motor Propellant
12	LOCV Due To Failure Of Left Side Near Main Landing Gear TPS, Consists Of 780 Tiles
13	LOCV Due To Failure Of Right Side Near Main Landing Gear (Fwd) TPS Consists Of 676 Tiles
14	LOCV Due To Catastrophic APU 2 Injector Leak On Entry
15	LOCV Due To Catastrophic APU 1 Injector Leak On Entry
16	LOCV Due To Catastrophic APU 3 Injector Leak On Entry
17	LOCV Due To Common Cause Failure Of All AC Inverters On Orbit
18	LOCV Due To Common Cause Failure Of All Fuel Cells On Orbit
19	LOCV Due To Failure Of The MPS Pneumatic System In Center SSME
20	LOCV Due To Failure Of The MPS Pneumatic System In Left SSME

Potential Risk Contributors for the DC-8 Agreement

1. *Cooperative Agreement Establishment* -establishing an acceptable cooperative agreement between NASA and UND
2. *Aircraft Transition* -physically transferring the aircraft to the UND facility
3. *Pilot Transition* -establishing trained pilots and providing NASA pilots as needed
4. *Maintenance Personnel Transition* -establishing trained maintenance personnel at UND
5. *Maintenance Program Transition* - establishing an acceptable maintenance program at UND
6. *Science Equipment Transition* -transferring the airborne science equipment to UND
7. *Aircraft Facility Acquisition* -acquiring an acceptable facility for the aircraft
8. *Fire Response Establishment* -establishing acceptable fire detection and suppression
9. *Security Services Establishment* -establishing acceptable security services
10. *Safety Program Establishment* -establishing an acceptable safety program at UND

Risk Matrix Categorization of the Contributors

1. Agreement
2. Aircraft
3. Pilot
4. Maintenance Personnel
5. Maintenance Program
6. Science Equipment
7. Aircraft Facility
8. Fire Response
9. Security
10. Safety Program



Consequences

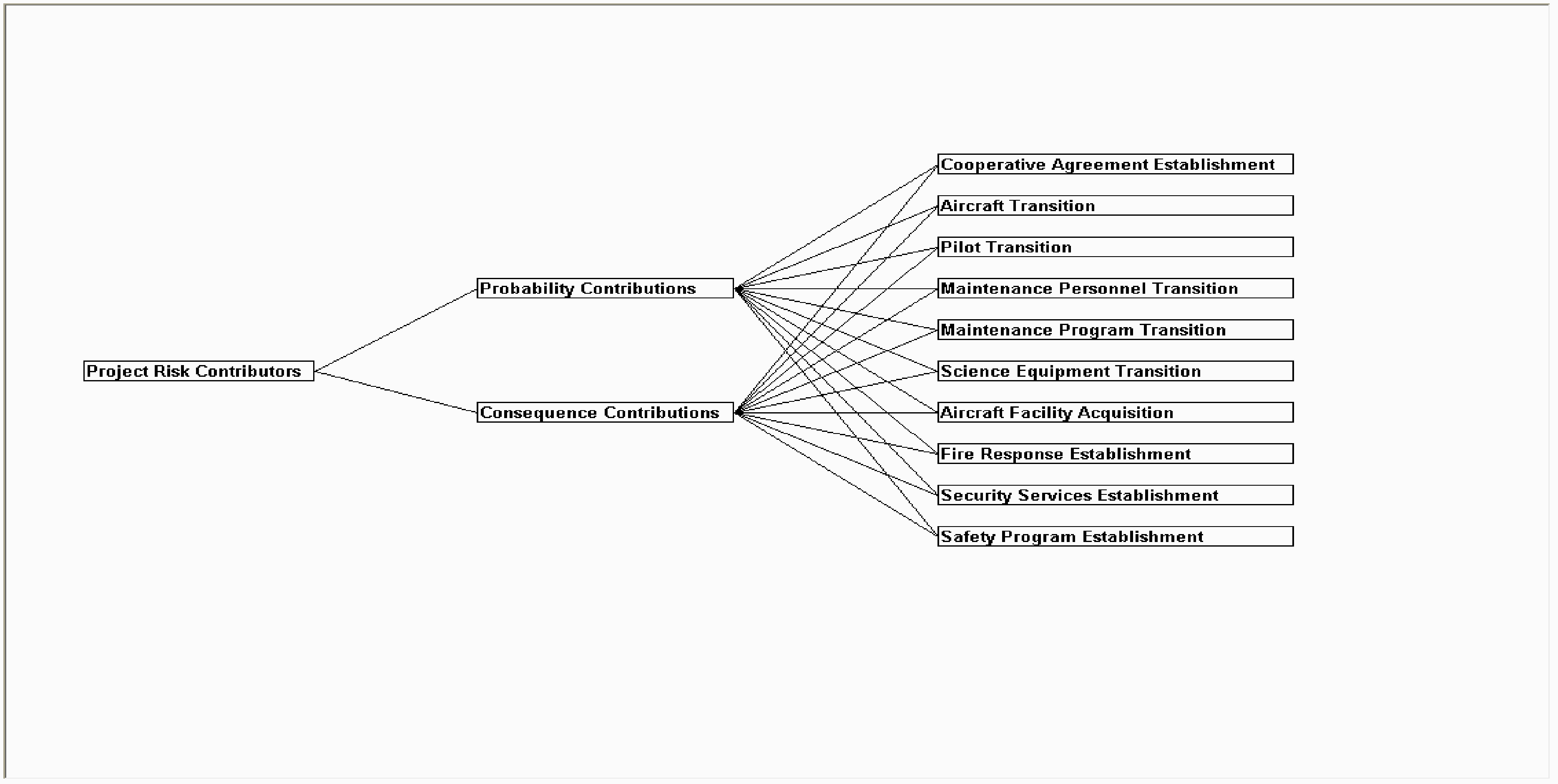
	1	2	3	4	5
5	🟩	🟨	🟨 2,3	🟥 8	🟥
4	🟩	🟩	🟨 10	🟨 4	🟥
3	🟩	🟩	🟨 5,6,7,9	🟨	🟨
2	🟩	🟩	🟩	🟨	🟨
1	🟩	🟩 1	🟩	🟩	🟨

Failure Probability

Relative Comparisons of the Contributor Probabilities and Consequences

		Failure	
Risk Contributors	**Failure Probability**	**Consequences**	**Risk**
1. Cooperative Agreement Establishment	1	1	1
2. Aircraft Transition	3	9	27
3. Pilot Transition	9	9	81
4. Maintenance Personnel Transition	9	9	81
5. Maintenance Program Transition	1	3	3
6. Science Equipment Transition	1	3	3
7. Aircraft Facility Acquisition	1	3	3
8. Fire Response Acquisition	9	9	81
9. Security Services Establishment	1	3	3
10. Safety Program Establishment	3	9	27

The Hierarchy Tree Identifying the Contributors



Project Risk Contributors

Probability Contributions

Consequence Contributions

Cooperative Agreement Establishment

Aircraft Transition

Pilot Transition

Maintenance Personnel Transition

Maintenance Program Transition

Science Equipment Transition

Aircraft Facility Acquisition

Fire Response Establishment

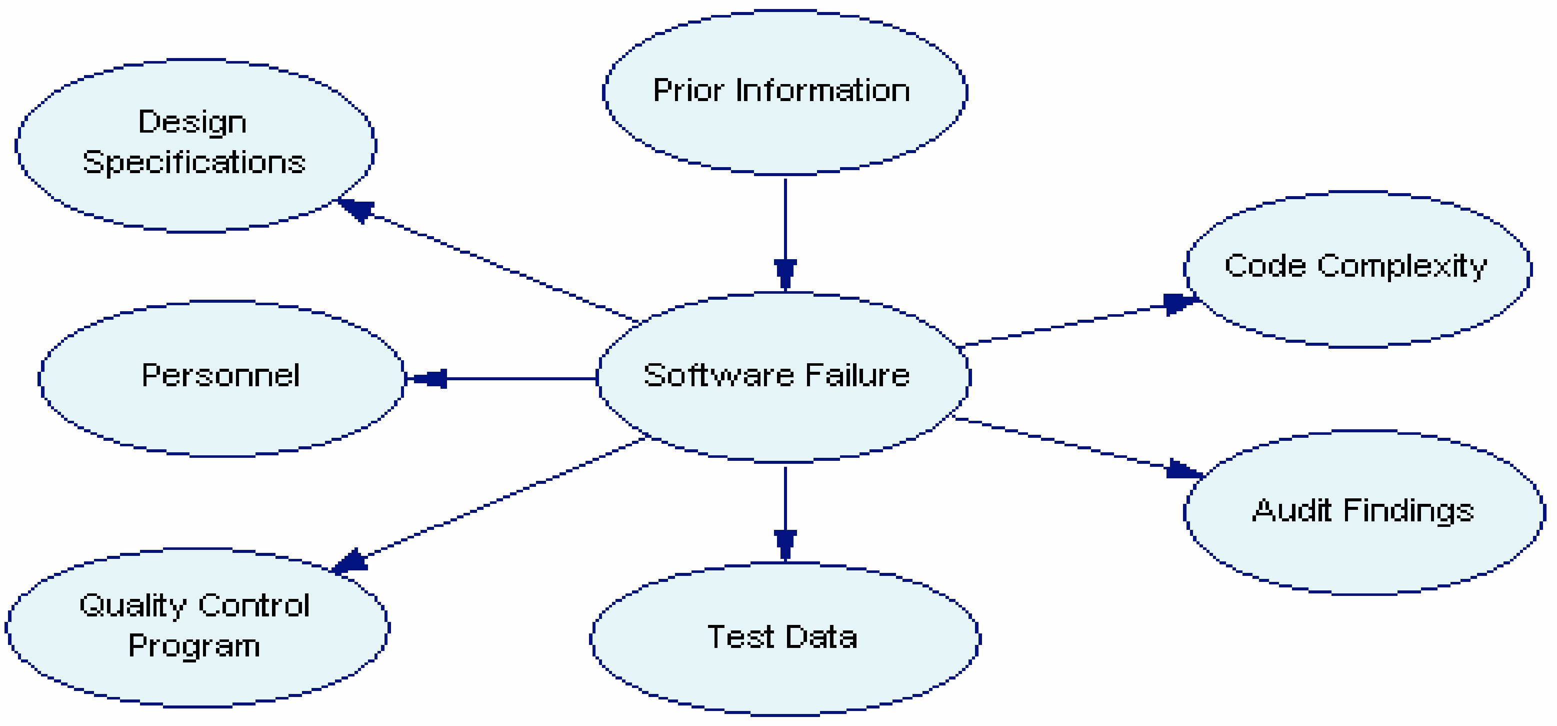
Security Services Establishment

Safety Program Establishment

Resulting Relative Probability, Consequence and Risk Contributions

Risk Contributors	Relative Failure Probability Contributions	Relative Failure Consequence Contributions	Relative Risk Contributions
1. Cooperative Agreement Establishment	2.6%	1.7%	0.3%
2. Aircraft Transition	7.9%	15.5%	8.7%
3. Pilot Transition	23.7%	15.5%	26.1%
4. Maintenance Personnel Transition	23.7%	15.5%	26.1%
5. Maintenance Program Transition	2.6%	5.2%	1.0%
6. Science Equipment Transition	2.6%	5.2%	1.0%
7. Aircraft Facility Acquisition	2.6%	5.2%	1.0%
8. Fire Response Acquisition	23.7%	15.5%	26.1%
9. Security Services Establishment	2.6%	5.2%	1.0%
10. Safety Program Establishment	7.9%	15.5%	8.7%
Total	100%	100%	100%

A Network of Factors Affecting Software Failure Probability



Probability of Observing Attributes for a Given Failure Probability Level

Software Failure Probability	High	Medium-High	Medium-Low	Low
Prior	0.1	0.3	0.3	0.3
Design Specs				
Well-defined	0.1	0.2	0.6	0.8
Some gaps	0.1	0.3	0.3	0.1
Vague	0.8	0.5	0.1	0.1
Personnel				
Experienced	0.1	0.2	0.6	0.8
Some experience	0.1	0.3	0.3	0.1
Little experience	0.8	0.5	0.1	0.1
Quality Control				
Comprehensive	0.1	0.2	0.6	0.8
Moderate	0.1	0.3	0.3	0.1
Minimal	0.8	0.5	0.1	0.1
Code Complexity				
High	0.7	0.5	0.5	0.3
Low	0.3	0.5	0.5	0.7
Audit Findings				
High marks	0.1	0.2	0.5	0.7
Medium marks	0.2	0.3	0.3	0.2
Low marks	0.7	0.5	0.2	0.1
Test Data				
Low failure rate	0.1	0.1	0.6	0.8
Moderate failure rate	0.1	0.6	0.3	0.1
High failure rate	0.8	0.3	0.1	0.1

Updated Probabilities for Different Possible Software Levels

Software Failure Probability	High	Medium-High	Medium-Low	Low
Prior	0.1	0.3	0.3	0.3
Design Specs				
Well-defined	0.02	0.12	0.37	0.49
Personnel				
Experienced	3.E-03	0.04	0.35	0.61
Quality Control				
Comprehensive	5.E-04	0.01	0.29	0.71
Code Complexity				
High	9.E-04	0.02	0.4	0.58
Audit Findings				
High marks	1.E-04	5.E-03	0.33	0.67
Test Data				
Low failure rate	2.E-05	7.E-04	0.27	0.73

Summary and Future Perspectives

- A spectrum of QRAs are carried out
- Gaps exist in methods and implementation
- Failure rate databases being assembled
- Procedure guides being written
- Decision guides being developed
- Tools and software being assembled